



A business advisory and advocacy law firm®

Colin M. Battersby  
Direct Dial: (248) 593-2952  
E-mail: [cbattersby@mcdonaldhopkins.com](mailto:cbattersby@mcdonaldhopkins.com)

RECEIVED

NOV 15 2021

CONSUMER PROTECTION

McDonald Hopkins PLC  
39533 Woodward Avenue  
Suite 318  
Bloomfield Hills, MI 48304

P 1.248.646.5070  
F 1.248.646.5075

November 10, 2021

**VIA U.S. MAIL**

John Formella  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: MA Federal Holdings, Inc. dba IGov Technologies, Inc. – Incident Notification**

Dear Mr. Formella:

McDonald Hopkins PLC represents MA Federal Holdings, Inc. dba IGov Technologies, Inc. (“IGov”). I am writing to provide notification of an incident that may affect the security of personal information of one (1) New Hampshire resident. IGov’s investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, IGov does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On September 30, 2021, IGov detected potential unauthorized access to its network. Upon learning of this issue, IGov contained and secured the threat, commenced a prompt and thorough investigation, and notified law enforcement. IGov immediately launched an investigation in consultation with outside cybersecurity professionals to help determine whether any sensitive data had been compromised because of the incident. IGov’s investigation determined that the unauthorized individual(s) potentially removed certain files and folders from portions of its network between September 27, 2021 and September 30, 2021. On October 21, 2021, following an extensive review and analysis of the data at issue, IGov determined that certain files and folders potentially removed from its network contained the resident’s full name and one or more of the following: Social Security number, financial account number, and/or taxpayer identification number.

At the time of this notification, IGov is not aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, out of an abundance of caution, IGov wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. IGov is providing the affected resident with written notification of this incident commencing on or about November 10, 2021 in substantially the same form as the letter attached hereto. IGov is offering the affected resident complimentary one-year membership with a credit monitoring service. IGov will advise the affected resident to always remain

November 10, 2021

Page 2

vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. IGov will advise the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies, and the Federal Trade Commission.

At IGov, protecting the privacy of personal information is a top priority. IGov is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. IGov continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (248) 593-2952 or [cbattersby@mcdonaldhopkins.com](mailto:cbattersby@mcdonaldhopkins.com).

Very truly yours,



Colin M. Battersby

Encl.



Dear [REDACTED]

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to iGov Technologies, Inc. ("iGov"). We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

On September 30, 2021, iGov detected unauthorized access to its network. Upon learning of this issue, iGov contained and secured the threat and commenced a prompt and thorough investigation. We launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to help determine whether any sensitive data had been compromised as a result of it. Our investigation determined that the unauthorized individual(s) had access to and potentially removed certain information from portions of our network between September 27, 2021 and September 30, 2021.

On October 21, 2021, following an extensive review and analysis of the data at issue, we determined that the information potentially removed from our network may have included your [REDACTED]

Given the unauthorized network access, potential acquisition of certain files and the value we place on our relationship with you, we wanted to notify you about this incident.

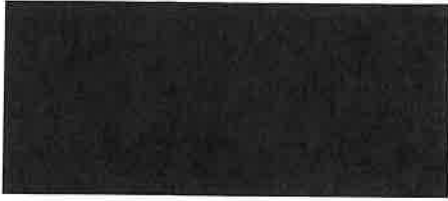
To date, we are not aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary one-year membership in Equifax® Credit Watch™ Gold. Equifax® Credit Watch™ Gold is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and Equifax® Credit Watch™ Gold, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, between 9:00 AM and 9:00 PM Eastern time.

Sincerely,



IGov Technologies, Inc.

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary 12-Month Credit Monitoring.**



Enter your Activation Code: [REDACTED]  
Enrollment Deadline: [REDACTED]

**Equifax Credit Watch™ Gold**

\*Note: You must be over age 18 with a credit file to take advantage of the product

**Key Features**

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications<sup>1</sup> when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts<sup>2</sup>, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock<sup>3</sup>
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft<sup>4</sup>

**Enrollment Instructions**

Go to [REDACTED]

Enter your unique Activation Code of [REDACTED] then click "Submit" and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click "Continue".

*If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.*

*Once you have successfully signed in, you will skip to the Checkout Page in Step 4*

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click 'Sign Me Up' to finish enrolling.

**You're done!**

The confirmation page shows your completed enrollment.

Click "View My Product" to access the product features.

<sup>1</sup>WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. <sup>2</sup>The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. <sup>3</sup>Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit [www.optoutprescreen.com](http://www.optoutprescreen.com). <sup>4</sup>The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued by Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



## 2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

### ***Equifax***

P.O. Box 105788  
Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>  
(800) 525-6285

### ***Experian***

P.O. Box 9554  
Allen, TX 75013

<https://www.experian.com/fraud/center.html>  
(888) 397-3742

### ***TransUnion LLC***

P.O. Box 6790  
Fullerton, PA 92834-6790

<https://www.transunion.com/fraud-alerts>  
(800) 680-7289

## 3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

### **Equifax Security Freeze**

P.O. Box 105788  
Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>  
1-800-349-9960

### **Experian Security Freeze**

P.O. Box 9554  
Allen, TX 75013

<http://experian.com/freeze>  
1-888-397-3742

### **TransUnion Security Freeze**

P.O. Box 2000  
Chester, PA 19016

<http://www.transunion.com/securityfreeze>  
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

## 4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **[www.annualcreditreport.com](http://www.annualcreditreport.com)**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

## 5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

**Maryland Residents:** You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**North Carolina Residents:** You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov/](http://www.ncdoj.gov/), Telephone: 877-566-7226.